AGENCY FOR DIGITAL GOVERNMENT

Den Danske Stat

OCES2 vs OCES3

OCES2 vs OCES3

Contents

1 Introduction

This document compares the structure of a OCES2 (Nets/NemID) certificate with the structure of a OCES3 (Den Danske Stat/MitID Erhverv) certificate. The new structure of OCES3 certificates is different from the existing OCES2 certificates and more compliant with European standards[1] on certificate content. OCES2 was developed before the European standards were developed and settled and did therefore not match the evolving standards.

Note that this document does not elaborate on qualified certificates, which is also part of the MitID Erhverv infrastructure.

Note also that personal OCES certificates are discontinued in the new infrastructure and replaced with qualified certificates.

This document does not describe the implemented services related to the certificate issuance and management like the fact that partial certificate revocation lists via LDAP is not supported in the new infrastructure.

1.1 Intended audience

The intended reader is a technical person, which are familiar with X.509 certificates and is responsible of adjusting existing applications using OCES2 certificates.

[1] ETSI EN 319 412-1, ETSI EN 319 412-2 and ETSI EN 319 412-5.

2 MOCES ("employee certificates")

2.1 Certificate content

2.1.1 Formalia

Field	MOCES2 (employee-cert)	MOCES3 (user-cert)	Remarks
X.509 version	3	3	No change[2]
SerialNumber			No change
Validity Period			No change
Signature algorithm	RSASSA-PKCS1-v1_5 with SHA-256	RSASSA-PSS with SHA-256[3]	
Trust anchor	TRUST2408	Den Danske Stat OCES rod-CA	
Public key	2048 bits RSA key	3072 bits RSA key	

2.1.2 Distinguished Name

Field	MOCES2	MOCES3	Remarks
country	DK	DK	No change
organizationName	Certificate subscribers organizational name and CVR number (UTF8String) in the form "OrgName // CVR:xxxxxxxx" where the OrgName is the registered name of the organization and xxxxxxxx is the CVR number	Certificate subscribers organizational name	The separator ' // ' and the CVR-number is not included in organizational name in MOCES3. For MOCES3 the CVR can be found in organisationIdentifier
organizationalUnit	Optional	No supported	
commonName	Certificate subjects name which may include the title e.g. "CEO John Doe"	Certificate subject's name or pseudonym	
givenName	N/A	Certificate subject's given name SHALL be present if surname is present. MUST not be present if pseudonym is present.	
surname	N/A	Certificate subject's surname SHALL be present if givenName is present. MUST not be present if pseudonym is present.	
pseudonym	N/A	Certificate subject's pseudonym	

[2] Note that ASN.1-wise this value is encoded as the value 2 since X.509 enumerates from 0.
[3] Note that CA certificates are using SHA-512

		MUST not be present if givenName and surname is present.	
organizationIdentifier	N/A	Certificate subscriber's CVR-number in the form NTRDK-XXXXXXXX where XXXXXXXX is the CVR-number of the organization.	
serialNumber	Unique identifier for the certificate subject in the form CVR:XXXXXXXX-RID:XXX..X	Unique identifier for the certificate subject in the form UI:DK-X:X:XXXXXXX..XX	Note that the X's in the MOCES3 is NOT the certificate subjects RID-number.
	Migrating from RID to UUID is supported by the supporting services API https://tu.nemlog-in.dk/oprettelse-og-administration-af-tjenester/log-in/hjaelp-og-vejledning/		

2.1.3 Extensions

Field	MOCES2	MOCES3	Remarks
keyUsage	digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	digitalSignature, contentCommitment, keyEncipherment	MOCES3 use profile F of ETSI EN 319 412-2 section 4.3.2
certificatePolicies	OID reference to MOCES2 policies + Link to repository + User notice referencing the underlying policy.	OID references to MOCES3 policies + OID reference to the compliant NCP policy	The link to repository and the user notice is discontinued
cRLDistributionPoints	HTTP link to CRL + LDAP path to a partial CRL	HTTP link to CRL	LDAP path to a partial CRL is discontinued. Full CRL or OCSP should be used as an alternative.
accessInformationAuthority	Reference to OCSP responder + Reference to the certificate of the CA which issued the certificate	Reference to OCSP responder + Reference to the certificate of the CA which issued the certificate	No change
authorityKeyIdentifier	Key identifier of the issuers public key corresponding to the private key used to sign a certificate	Key identifier of the issuers public key corresponding to the private key used to sign a certificate	No change

subjectKeyIdentifier	Key identifier of the subject's public key included in the certificate	Key identifier of the subject's public key included in the certificate	No change
basicConstraints	cA: FALSE	cA: FALSE	No change
subjectAlternativeName	If present it includes the subjects e-mail address	If present it includes the subjects e-mail address	No change
qcStatement-2	Not present	semanticsIdentifier: semanticsIdentifier: id-etsi-qcs-semanticsId-Natural nameRegistrationAuthorities: https://uid.gov.dk	

3 VOCES (organizational certificates)

3.1 Certificate content

3.1.1 Formalia

Field	VOCES2	VOCES3 – VOCES profile	Remarks
X.509 version	3	3	No change[4]
SerialNumber			No change
Validity Period			No change
Signature algorithm	RSASSA-PKCS1-v1_5 with SHA-256	RSASSA-PSS with SHA-256[5]	
Trust anchor	TRUST2408	Den Danske Stat OCES rod-CA	
Public key	2048 bits RSA key	3072 bits RSA key	

3.1.2 Distinguished Name

Field	VOCES2	VOCES3 – VOCES profile	Remarks
country	DK	DK	No change
organizationName	Certificate subscribers organizational name and CVR number (UTF8String) in the form “OrgName // CVR:xxxxxxxx” where the OrgName is the registered name of the organization and xxxxxxxx is the CVR number	Certificate subscribers organizational name	The separator ‘ // ‘ and the CVR-number is not included in organizational name in VOCES3. For VOCES3 the CVR can be found in organisationIdentifier
organizationalUnit	Optional	No supported	
commonName	organizations name optional organization unit names and optional function description		
organizationIdentifier	N/A	Certificate subscriber’s CVR-number in the form NTRDK-XXXXXXXX where XXXXXXXX is the CVR-number of the organization.	
serialNumber	Unique identifier for the certificate subject in the form CVR:XXXXXXXX-UID:XXX..X	Unique identifier for the certificate subject in the form UI:DK-X:X:XXXXXXX..XX	Note that the X’s in the MOCES3 is NOT the certificate subjects UID-number.

[4] Note that ASN.1-wise this value is encoded as the value 2 since X.509 enumerates from 0.
[5] Note that CA certificates are using SHA-512

3.1.3 Extensions

Field	VOCES2	VOCES3 – VOCES profile	Remarks
keyUsage	contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	digitalSignature, contentCommitment, keyEncipherment	VOCES3 use profile F of ETSI EN 319 412-2 section 4.3.2
certificatePolicies	OID reference to VOCES2 policies + Link to repository + User notice referencing the underlying policy.	OID references to VOCES3 policies + OID reference to the compliant NCP policy	The link to repository and the user notice is discontinued
cRLDistributionPoints	HTTP link to CRL + LDAP path to a partial CRL	HTTP link to CRL	LDAP path to a partial CRL is discontinued
accessInformationAuthority	Reference to OCSP responder + Reference to the certificate of the CA which issued the certificate	Reference to OCSP responder + Reference to the certificate of the CA which issued the certificate	No change
authorityKeyIdentifier	Key identifier of the issuers public key corresponding to the private key used to sign a certificate	Key identifier of the issuers public key corresponding to the private key used to sign a certificate	No change
subjectKeyIdentifier	Key identifier of the subject's public key included in the certificate	Key identifier of the subject's public key included in the certificate	No change
basicConstraints	cA: FALSE	cA: FALSE	No change
subjectAlternativeName	If present it includes the subjects e-mail address	If present it includes the subjects e-mail address	No change
qcStatement-2	Not present	semanticsIdentifier: semanticsIdentifier: id-etsi-qcs-semanticsId-Legal nameRegistrationAuthorities: https://uid.gov.dk	

4 FOCES (Functional certificates)

Note that FOCES certificate policies are discontinued and in the OCES3 infrastructure FOCES is just a profile under the VOCES certificate policy.

4.1 Certificate content

4.1.1 Formalia

Field	FOCES2	VOCES3 – FOCES profile	Remarks
X.509 version	3	3	No change[6]
SerialNumber			No change
Validity Period			No change
Signature algorithm	RSASSA-PKCS1-v1_5 with SHA-256	RSASSA-PSS with SHA-256[7]	
Trust anchor	TRUST2408	Den Danske Stat OCES rod-CA	
Public key	2048 bits RSA key	3072 bits RSA key	

4.1.2 Distinguished Name

Field	FOCES2	VOCES3 – FOCES profile	Remarks
country	DK	DK	No change
organizationName	Certificate subscribers organizational name and CVR number (UTF8String) in the form “OrgName // CVR:xxxxxxxx” where the OrgName is the registered name of the organization and xxxxxxxx is the CVR number	Certificate subscribers organizational name	The separator ‘ // ‘ and the CVR-number is not included in organizational name in VOCES3. For VOCES3 the CVR can be found in organisationIdentifier
organizationalUnit	Optional	No supported	
commonName	organizations name optional organization unit names and optional function description		
organizationIdentifier	N/A	Certificate subscriber’s CVR-number in the form NTRDK-XXXXXXXX where XXXXXXXX is the CVR-number of the organization.	
serialNumber	Unique identifier for the certificate subject in the form CVR:XXXXXXXX-UID:XXX..X	Unique identifier for the certificate subject in the form UI:DK-X:X:XXXXXXX..XX	Note that the X’s in the MOCES3 is NOT the certificate subjects UID-number.

[6] Note that ASN.1-wise this value is encoded as the value 2 since X.509 enumerates from 0.
[7] Note that CA certificates are using SHA-512

4.1.3 Extensions

Field	FOCES2	VOCES3 – FOCES profile	Remarks
keyUsage	contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	digitalSignature, keyEncipherment	VOCES3 use profile D of ETSI EN 319 412-2 section 4.3.2
certificatePolicies	OID reference to VOCES2 policies + Link to repository + User notice referencing the underlying policy.	OID references to VOCES3 policies + OID reference to the compliant NCP policy	The link to repository and the user notice is discontinued
cRLDistributionPoints	HTTP link to CRL + LDAP path to a partial CRL	HTTP link to CRL	LDAP path to a partial CRL is discontinued
accessInformationAuthority	Reference to OCSP responder + Reference to the certificate of the CA which issued the certificate	Reference to OCSP responder + Reference to the certificate of the CA which issued the certificate	No change
authorityKeyIdentifier	Key identifier of the issuers public key corresponding to the private key used to sign a certificate	Key identifier of the issuers public key corresponding to the private key used to sign a certificate	No change
subjectKeyIdentifier	Key identifier of the subject's public key included in the certificate	Key identifier of the subject's public key included in the certificate	No change
basicConstraints	cA: FALSE	cA: FALSE	No change
subjectAlternativeName	Not present	If present it includes the subjects e-mail address	No change
qcStatement-2	Not present	semanticsIdentifier: semanticsIdentifier: id-etsi-qcs-semanticsId-Legal nameRegistrationAuthorities: https://uid.gov.dk	

5 CRL

5.1 CRL content

5.1.1 Formalia

Field	OCES2	OCES3	Remarks
X.509 version	2	2	No change[8]
SerialNumber			No change
thisUpdate			No change
nextUpdate			No change
Signature algorithm	RSASSA-PKCS1-v1_5 with SHA-256	RSASSA-PSS with SHA-512	
Trust anchor	TRUST2408	Den Danske Stat OCES rod-CA	

5.1.2 Extensions

Field	OCES2	OCES3	Remarks
CRL Number			No change
authorityKeyIdentifier	Key identifier of the issuers public key corresponding to the private key used to sign a certificate	Key identifier of the issuers public key corresponding to the private key used to sign a certificate	No change
expiredCertificatesOnCRL	Not present	The inclusion of this extension indicates that the revocation information contains information about revoked certificates since the date described in the time.	

[8] Note that ASN.1-wise this value is encoded as the value 1 since X.509 enumerates from 0.

6 More information

The full specification of OCES3 certificates and CRL can be found at the repository of the OCES3 trust provider “Den Danske Stat” at https://ca1.gov.dk.